D4, end

creating, responsive to the initial URL call, the session identifier; and

returning the session identifier to the client for storage by the client for use in each URL call to the server system.

REMARKS

Claims 3, 5-26, 31-43, 49-63, 67-93, 96-98, 100-106 and 108-111 are pending in the application. All claims have been rejected.

Incorporation by reference to Payne patent

The Examiner states that Applicants' attempt to incorporate subject matter into this application by reference to Payne et al., U.S. Patent No. 5,715,314, corresponding to U.S. Application S/N 08/328,133, is improper because it is not accompanied by an affidavit or declaration executed by Applicants. Office Action, paragraph 3, page 2.

However, the MPEP states that "if a copy of a printed U.S. patent is furnished, no affidavit or declaration is required." MPEP, section 608.01(p).I.A.1. Therefore, as a copy of the Payne patent is attached hereto, Applicants do not believe an affidavit or declaration is required.

The claimed invention

Applicants' invention uses a "session identifier" or SID to provide a "session" of communications between a client system and a server system in a "stateless" session environment. An SID containing enough information to support a session is appended to the initial and subsequent requests. This information can include, for example, an authorization identifier, a user identifier, an accessible domain, a key identifier, an expiration time, a date, the IP address of the user computer, and/or an unforgeable digital signature "such as a cryptographic hash of all of the other items in the SID encrypted with a secret key." Specification as filed, page 6, lines 16-21. The present invention is particularly suited to restricting access to server sites on the World Wide Web.

A user's user name and password is verified once, at the beginning of a session, and a SID is created upon verification. The server does not need to perform password verification for each access within a session of requests. Rather, upon each request containing a SID, the server simply checks whether the SID is valid. Such validation may include, for example, the following checks:

> (1) the SID's digital signature is compared against the digital signature computed from the remaining items in the SID and the user IP address using the secret key shared by the authentication and content servers; (2) the domain field of the SID is checked to verify that it is within the domain authorized; and (3) the EXP field of the SID is checked to verify that it is later than the current time.

Specification as filed, page 12, lines 5-13.

In one embodiment, for example, "a valid SID allows the client to access all controlled files within a protection domain without requiring further authorization." Specification as filed, page 7, lines 1-3. That is, information regarding access rights is fully contained within the SID, and need not be reentered by a user attempting to access *any* file within a domain for which the user's authorization has already been verified.

Upon receiving the SID from the server system, the client browser stores the SID. The client browser then appends the stored SID to each subsequent request to that server system. Because just the SID (and not the entire request) is stored, and because the SID is appended to subsequent requests to the particular server, use of the SID is not limited merely to a particular request but rather can extend to all subsequent requests to the server system, thus providing the sense of a session between the client and the server system.

Independent Claims 3, 35 and 79 have been amended for clarity. Support for these amendments can be found, for example, at page 5, line 27 to page 6, line 2, and at page 8, lines 12-19 of the Specification as filed.

Freeman-Benson

Freeman-Benson teaches protection of a private document using a "special URL" which contains an access key consisting of an encrypted login name and password, Freeman-Benson, para. 9, page 2, entered by the user from a login page. "If the password is correct, the server returns a Web page containing a link to the private information. The URL for this link includes the encrypted access key." Freeman-Benson, para. 11, pages 2-3.

The special URL does not provide the sense of a session. For example, the special URL can be shared by others, or stored in a hotlist for later use, providing access to a particular document until the password is changed, at which time the special URL is no longer valid. Freeman-Benson, para. 12, page 3. Furthermore, the special URL will again be valid if the password is changed back. Freeman-Benson, footnote 1, page 5.

By storing the special URL, for example, in a hotlist, Freeman-Benson stores a particular request, complete with URL, user name and password. Such a mechanism can provide automatic validation for the particular request, but cannot easily be extended to other requests to the same server using different URLs. Should the user make a different request to the same server, the user must again be prompted for user name and password. In other words, Freeman-Benson does not teach a client that stores some entity, e.g., a SID or other tag, that is appended to subsequent distinct requests to a particular server.

Johnson

Johnson teaches a credentials identifier which is used to reference a credentials structure stored in a server. The client must have certain knowledge about credentials identifiers before commencing any communication with the server. Initially, the client sends a "request for service" which includes authorization information. The server builds a credentials record in response to the request, and returns to the client a credentials identifier associated with the newly created credentials record. When the client presents the credentials identifier in subsequent requests, the server uses the credentials identifier to retrieve the credentials record, and from the credentials record validates the request. Access rights are stored on the server itself, in the credentials record, and are not included in the credentials identifier. See, for example, Johnson, column 5, lines 50-65.

Claims 3, 5-6, 13-14, 23, 25, 31-32, 35-38, 49-54, 56-62, 67-74, 77, 79-85, 87-93, 101-102, 104, 106 and 108-111

Claims 3, 5-6, 13-14, 23, 25, 31-32, 35-38, 49-54, 56-62, 67-74, 77, 79-85, 87-93, 101-102, 104, 106 and 108-111 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman-Benson in view of Johnson et al., U.S. Patent No. 5,560,008 ("Johnson"). Office Action, para. 5, page 2.

With respect to Claim 3, the Examiner equates Freeman-Benson's "specialized URL" and Johnson's "credential identifier" with Applicants' session identifier. Office Action, para. 6, page 3.

However, Applicants respectfully assert that neither Freeman-Benson's specialized URL nor Johnson's credentials identifier is equivalent to a session identifier as recited in Applicants' Claim 3.

For example, Freeman-Benson teaches a "specialized URL" containing an access key which is simply an encrypted login name and password. Furthermore, Freeman-Benson teaches storing the specialized URL, that is, the request (the normal URL) along with the access key. Thus, later use of this stored specialized URL will result in a repetition of the original request, without requiring further authorization. Freeman-Benson does not append the specialized URL to subsequent requests - doing so would result in a meaningless request: one URL appended by another URL.

Applicants' invention, on the other hand, stores the SID and appends the stored SID to each URL or request to the particular server that provided the SID, thus defining a session. That is, subsequent requests to the server from the browser do not require the user to enter additional verification information, even for different requests, because the SID which accompanies each request provides validation.

In addition, Freeman-Benson, at the time of its publication, worked with "*all* existing WWW browsers." Freeman-Benson, paragraph 26, page 5, original emphasis. Such browsers as existed at that time would not support Applicants' claimed invention, which, as of the priority date, required a modified browser. See Specification as filed, page 8, lines 15-19. Of course, "modern" browsers which support cookies are such "modified" browsers.

Thus, Freeman-Benson does not teach or suggest "returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent distinct requests to the server system; and appending the stored session identifier to each of the subsequent distinct requests from the client to the server system," as recited in amended Claim 3.

The Examiner further asserts that Johnson teaches "appending a session identifier to subsequent service requests...." Office Action, para. 6, page 3. Again, Applicants disagree.

Johnson does not teach or suggest a session identifier but rather teaches a credentials identifier. A credentials identifier is a "small value" used to access a "credentials structure" which is maintained on the server. See Johnson, column 5, lines 54-65. Each time a request is made, the server reconstructs "an image of the user." Johnson, column 5, lines 40-42. Johnson uses the credentials identifier to locate the credentials structure from which the image of the user is reconstructed.

Applicants' invention, on the other hand, does not need to perform this reconstruction, because the session identifier itself contains sufficient information to validate that the request is authorized.

Neither Freeman-Benson nor Johnson, separately or in combination, teach or suggest "returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent distinct requests to the server system; and appending the stored session identifier to each of the subsequent distinct requests from the client to the server system," as recited in Claim 3. Therefore, Applicants respectfully request that Claim 3 be allowed.

The Examiner makes substantially the same arguments with respect to Claim 35, Office Action, para. 15, page 5, and to Claim 79, Office Action, para. 32, pages 8-9. For the same reasons discussed above, Claims 35 and 79 should be allowable.

Allowance of all other claims, i.e., Claims 5-26, 31-34, 36-43, 49-63, 67-78, 80-93, 96-98, 100-106 and 108-111, which depend from one of Claim 3, Claim 35 or Claim 79, should follow.

Claims 7-12, 24-26, 33-34, 39-43, 55, 76, 78 and 86

Dependent Claims 7-12, 24-26, 33-34, 39-43, 55, 76, 78 and 86 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman-Benson and Johnson further in view of Filepp et al., U.S. Patent No. 5,347,632 ("Filepp"). Allowance of these dependent claims should follow from the independent claims from which they depend, i.e., Claims 3, 35 and 79, discussed above.

With respect to Claim 26 in particular, the Examiner asserts both that Johnson teaches "wherein the session identifier comprises a user identifier," and that Filepp teaches "charging the user identified ... for access to the document." Office Action, para. 50, pages 12-13.

However, Johnson teaches only that a credentials identifier contains a count and an index, the index for retrieving the corresponding set of credentials from a credentials table. Johnson, column 8, lines 6-10. While the set of credentials within Johnson's credentials *structure* contains a user id, this user id is not part of the request sent from the client to the server. Johnson does not teach or suggest "wherein the session identifier comprises a user identifier," as recited in Claim 26.

Furthermore, Filepp teaches "the purchase of items such as retail merchandise and groceries...," but does not teach or suggest "charging the user identified in the identifier for access to the [requested] document," as recited in Claim 26.

Therefore, Claim 26 should be allowable in its own right.

Claims 15-21, 63 and 75

Dependent Claims 15-21, 63 and 75 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman-Benson and Johnson further in view of Cheng et al., U.S. Patent No. 5,544,322 ("Cheng"). Office Action, para. 56, page 14. Allowance of these dependent claims should follow from independent Claim 3 from which they directly or indirectly depend, discussed above.

Claim 22

Claim 22 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman-Benson, Johnson, Cheng further in view of Filepp. Office Action, para. 67, page 16. Allowance of dependent Claim 22 should follow from independent Claim 3 from which Claim 16 indirectly depends.

Claims 96-98, 100, 103 and 105

Claims 96-98, 100, 103 and 105 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman-Benson in view of Dedrick, U.S. Patent No. 5,768,521 ("Dedrick"). Office Action, para. 69, page 17. Allowance of these dependent claims should follow from independent Claim 3 from which they directly or indirectly depend.

On the Examiner's motivation to combine references

In offering motivation to combine Benson-Freeman with Johnson and other references, see for example, Office Action, paras. 39-41, page 10; para. 55, page 14; para. 66, page 16; para. 68, page 17; and para. 76, page 19, the Examiner has actually supplied motivation for advancing the state of the art. Advancing the state of the art is what drives most if not all invention. However, the Examiner has not provided "clear and particular" motivation to combine the references. See Winner International Royalty Corporation v. Ching-Rong Wang, 53 USPQ2d 1580, 1586 (Fed. Cir. 2000), *cert. denied,* 120 SC 2679 (U.S. June 12, 2000), citing In re Dembiczak, 175 F.3d 994, 1000, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Freeman-Benson is directed to World Wide Web applications using URLs and HTTP. Freeman-Benson, para. 1, page 1. As is well-known, the Web is normally a stateless environment; that is, each access or request is independent of all other requests. In attempting to relieve a user of the necessity of having to re-enter a login name and password each time a particular protected document is requested, Freeman-Benson circumnavigates this statelessness by adding the login name and password, in encrypted form, to the original URL, thus forming a "special URL."

Johnson, on the other hand, employing a stateful server, teaches away from using a stateless environment in the first place, by passing back and forth a credentials identifier that points to a credentials record stored in the server. For example, "[t]he ... strategies described here cannot be implemented unless the server keeps such state information." Johnson, column 2, lines 55-65.

The Examiner has asserted that, regarding Claims 1 and 79 for example (and presumably Claim 35 as well), it would have been obvious "that substituting Johnson's appending a session identifier to subsequent request in Freeman-Benson's system for accessing a private web database would have improved system effectiveness. The motivation would have been to improve upon Freeman-Benson method of authentication by incorporating authorization." Office Action, para. 41, pages 10-11.

As noted above, however, improving effectiveness, i.e., advancing the state of the art, is a typical goal of every invention and does not per se provide a motivation to combine specific references.

Even if Freeman-Benson were combined with Johnson, however, the end result would not be Applicants' claimed invention. That is, a "special URL" containing an encrypted user name and password, combined with a credentials identifier that points to a credentials record stored on a server, is not equivalent to a session identifier that is returned "from the server system to the client, the client storing the session identifier for use in subsequent requests to the server system [where the] the stored session identifier [is appended] to each of the subsequent requests from the client to the server system," as recited in amended Claim 3.

Therefore, Applicants believe that the rejections of Claims 3, 35 and 79 based on the combination of Freeman-Benson and Johnson is improper. The Examiner has made similar assertions regarding motivation for combining references. See, for example, Office Action, paras. 39-40, page 10; para. 55, page 14; para. 66, page 16; para. 68, page 17; and para. 76, page 19. Applicants therefore respectfully request that the Examiner withdraw claim rejections based on 35 U.S.C. 103(a), on this basis as well as on the basis of the substantive arguments made under the previous headings.

Claims 38-43, 68-74, 77-78 and 80-93

As noted by the Examiner, Office Action, paras. 77-80, page 20, the language of these claims is substantially equivalent to claims already discussed. Therefore, for reasons discussed above, these Claims 38-43, 68-74, 77-78 and 80-93 should be allowable.

New Claims 112 - 115

New claims 112 - 115 recite Applicants' invention, as described above, from the viewpoint of the server system. No new matter has been introduced.

CONCLUSION

In view of the above amendments and remarks, it is believed that all pending claims, i.e., Claims 3, 5-26, 31-43, 49-63, 67-93, 96-98, 100-106 and 108-115, are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned at (781) 861-6240.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By____________________
Gerald M. Bluhm
Registration No. 44,035
Telephone (781) 861-6240
Facsimile (781) 861-9540

Lexington, Massachusetts 02421-4799
Dated: 12/28/01

MARKED UP VERSION OF AMENDMENTS

Claim Amendments Under 37 C.F.R. § 1.121(c)(1)(ii)

3. (Three Times Amended) A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent [communications] distinct requests to the server system; and

appending the stored session identifier to each of the subsequent [service] distinct requests from the client to the server system [within a session of requests].

35. (Three Times Amended) An information system on a network, comprising:

means for receiving service requests from a client [clients] and for determining whether a service request includes a session identifier, wherein communications to and from the client [clients] are according to hypertext transfer protocol;

means for providing the session identifier in response to an initial service request from the client in a session of requests;

means for storing, at the client, the session identifier for use in each communication to the server system;

means for appending the stored session identifier to each of [servicing] subsequent communications [service requests within the session of requests] from the [a] client to the server system [, the subsequent service requests including the session identifier]; and

means for servicing the subsequent service requests [storing, at the client, the session identifier for use in each communication associated with the document request].

79. (Twice Amended) A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent communications; and

at the client, appending as part of a path name in a uniform resource locator the stored session identifier to each subsequent service request [requests] from the client to the server system within a session of requests.